EXHIBIT A (REDACTED)

Expert Declaration In The Matter Of:

United States of America

v.

Thomas C. Goldstein

Criminal No. LKG-25-0006

Prepared By:
Jason Trager
Senior Director
Blockchain and Digital Assets
FTI Consulting
1166 Avenue of the Americas | 16th Floor
New York, NY 10036

Date:
February 27, 2025

Prepared For:
Munger, Tolles & Olson LLP
Counsel for Thomas C. Goldstein

TABLE OF CONTENTS

Page

Statement of Qualifications

1. I, Jason Trager, am a Senior Director at FTI Consulting Technology LLC ("FTI") in the Blockchain and Digital Assets practice of its Technology segment. FTI's Technology segment provides blockchain advisory services, cryptocurrency investigations, digital asset investigations, and electronic discovery services to assist organizations across a variety of industries to better govern, secure, find, and analyze information. As a Senior Director within the practice, I have overseen investigations into large scale hacks of cryptocurrency from individuals and corporate entities, conducted due diligence into web3 companies, and evaluated policies and procedures concerning money laundering and illicit activities.

2. I was previously employed by BNP Paribas as Vice President of the Financial Investigations Unit for North America and operated within the bank's Digital Assets Group. As a financial security officer for BNP Paribas, I served as their subject matter expert concerning digital assets, illicit activity, and BSA/AML compliance. I advised transaction monitoring teams on the use of blockchain analytics and developed policies and procedures concerning exposure to illicit activity. I consulted investment groups on the purchase and sale of digital assets, worked with product development teams to secure newly tokenized assets, and issued briefs to attorneys, compliance officers, and executives on regulatory developments and enforcement actions that concerned digital assets. I was the lead AML advisor on the bank's first digital bond issuance and helped author a guide to the rules and procedures of notifying U.S. regulatory agencies regarding digital asset activity. I also designed the bank's digital assets risk assessment.

3. Prior to my employment with BNP Paribas, I was the Chief of Cyber Crimes for the Queens County District Attorney's Office of New York City. I co-created the Office's Cryptocurrency Task Force where I worked with investigators from Homeland Security Investigations, the FBI Cyber Crime Unit, and the NYPD Computer Crimes Unit. I oversaw over twenty digital asset investigations concerning the theft of digital assets, money laundering through cryptocurrency, ransomware, and illegal trafficking through darknet markets. Utilizing blockchain tracing and digital forensics, these investigations resulted in the successful prosecution of illicit actors, and the seizure of digital assets valued at hundreds of thousands of dollars.

4. I am a member of the Association of Certified Anti-Money Laundering Specialists (ACAMS), which is the largest membership organization dedicated to enhancing the knowledge and skills of financial crime detection and prevention worldwide. I have completed course work and passed the required examinations administered by ACAMS to be certified as a Crypto-asset Anti-Financial Crimes Specialist. I am a member of the Blockchain Council, an organization that provides training and certification in technical specialties. Through the Blockchain Council I have been designated as a Certified Cryptocurrency Expert and Certified Blockchain Expert. I have been trained by blockchain analytics firm Chainalysis as a cryptocurrency investigator and have achieved the designation of an Investigation Specialist. I am also a member of the Wall Street Blockchain Alliance, an industry leading non-profit trade association that guides and promotes comprehensive adoption of blockchain technology across global markets. I have lectured to legal and law enforcement communities in the United States and Canada on the topics of cryptocurrency, blockchain

investigations, digital asset evidence, and cybercrime. I hold a J.D. from Brooklyn Law School and a bachelor's degree from the University of Maryland. My curriculum vitae is attached hereto as Exhibit A.

Scope of Engagement

5. I have been retained to provide expert opinions on the following:

- The mechanisms underpinning blockchain technology and digital assets
- Transparency of blockchain transactions and crypto wallets
- Risks and best practices concerning transacting cryptocurrency
- The ability to own and control cryptocurrency wallets
- An analysis of the transaction activity of public addresses [redacted]54E3 ("54E3") and [redacted]935B ("935B")

6. I have been retained as a testifying expert at the rate of $711.00 per hour. My fee is not contingent on the outcome of this case.

7. All of my opinions and conclusions presented in this report are held to a reasonable degree of professional certainty. I prepared my report while employed by FTI Consulting. I reserve the right to update or change my opinions if new information is made available to me in the future.

Understanding the Blockchain

8. The blockchain is a decentralized, digital network that operates as a digital ledger recording all transactions in real time. It consists of records, called blocks, that are used to record transactions. Blocks are created and attached to the chain by multiple nodes within the network. Nodes are computers that participate in the network by verifying and confirming new data through a process of consensus.[1]

9. As each block is recorded on a blockchain, a cryptographic hash, or unique digital fingerprint, of the prior block is recorded as part of it. Blocks are linked together in the chain in this manner. What results is the blockchain.

10. The data stored on the blockchain is protected, as it is stored in a decentralized and cryptographically secure manner with multiple duplicate copies across the network. The data is also immutable as it is created through consensus by multiple nodes. Once data is recorded on a blockchain it cannot be altered.

Cryptocurrencies

11. Cryptocurrencies are digital mediums of value that are transacted on the blockchain and integrate cryptography to manage transactions. There are several types of cryptocurrencies, and depending on the kind of cryptocurrency, the value may be variable

[1] https://www.gao.gov/assets/gao-19-704sp.pdf

or set. For instance, the value of a stablecoin cryptocurrency is pegged to the value of fiat currency or a physical asset. By example, in the case of stablecoins USDT and USDC, the value of each token is pegged to the value of the US dollar. However, the value of a cryptocurrency like bitcoin or ETH is based simply on the laws of supply and demand.[2]

Public and Private Nature of Crypto Accounts

12. I am aware that it has been suggested in these proceedings that it is impossible to know how much cryptocurrency is held in any particular cryptocurrency account at this moment. That suggestion is incorrect. By intent and design, blockchains such as Bitcoin and Ethereum operate as public networks. The decentralized and permissionless nature of these blockchains means that anyone can view, verify, or participate in the transaction process.[3] As a result, the amount of cryptocurrency held in a particular account at any given time is publicly-available information.

13. This also means that activity associated with a specific public address can be reviewed by outside observers. Using open source blockchain explorers or proprietary blockchain forensics software provides the ability to review an account's transaction history. The information available includes which cryptocurrencies or tokens were sent or received, what amount of funds were moved, which public addresses were involved in each transaction, and when the transactions occurred. Some of the most well known open source blockchain explorers include Blockchain.com, Etherscan (https://etherscan.io/), and Solscan (https://solscan.io/).

14. Even with blockchain data open to public view, a degree of privacy remains through the use of public addresses or public keys. A public address is a unique alphanumeric identifier that is associated with a crypto wallet. The length of a public address often depends on the network. For example, an Ethereum-based address will be 42 characters long, beginning with 0x and followed by a unique 40-character string.[4] This public address is the only public data that represents the actual owner of the wallet on the blockchain. Therefore, it is impossible to know who is behind the sending or receiving of cryptocurrency simply by looking at blockchain records. Instead, sources outside the blockchain must provide the information necessary to know who owns or controls that account. [5]

Transacting on the Blockchain

15. Digital assets are traded on the blockchain through use of public and private keys. The public key, or wallet address, is a pseudo-anonymous identifier used to receive cryptocurrency. This address is what is observable on the blockchain, and it acts as the address to which a transaction is sent. The address of both the sender and recipient are publicly observable, but the actual identity of either the sender or recipient is not. The private key grants control over the cryptocurrency associated with the public key. A transaction is initiated when a sender utilizes their *private key* to direct an amount of

[2] https://www.kraken.com/learn/types-of-cryptocurrency
[3] https://www.lcx.com/introduction-to-public-blockchain/
[4] https://info.etherscan.com/what-is-an-ethereum-address/
[5] Examples of such sources include Know Your Customer information from centralized entities or public admissions from wallet owners

cryptocurrency to be sent to a recipient's *public address*. For illustration, a public key is analogous to an e-mail address, and a private key is analogous to the password to that e-mail address. Accordingly, when a user sends the *public address* of a wallet to a third party so that the third party can make a payment into the wallet, the user does not thereby grant the third party the ability to control the funds in the wallet. To exercise that control, the *private key* is required.

16. When a transaction is initiated, a small fee is required to process the transaction. This transaction fee, or gas fee, is necessary to get the transaction included in the block data and verified. Fees are paid to the participants that verify the block that contains that particular transaction.[6] In my experience, it is very common for cryptocurrency users to reduce transaction fees by minimizing the number of transactions necessary to send crypto to the intended recipient. For instance, in a situation where user A needs to send an amount of cryptocurrency to user B, and user B needs to send an amount of crypto to user C, user A sending cryptocurrency directly to user C is the fastest and most efficient method and will result in fewer gas fees.

17. Moreover, sending cryptocurrency in this manner (*i.e.*, directly from user A to user C, instead of from user A to user B and then user B to user C), protects against the dangers of sending to an incorrect address. A primary benefit of the blockchain is that transactions are initiated immediately and completed quickly. However, transactions cannot be canceled once initiated. Once the transaction is confirmed, it becomes permanently and immutably recorded on the blockchain and secured by cryptographic signature. This renders the transaction irreversible. Therefore, it is crucial that users of cryptocurrency ensure that they are sending assets to the correct public address before initiating a transaction.

18. Each time a user initiates a transaction there is a risk that funds can be lost by inputting the wrong address by mistake. If a user enters an address in error, the funds will be sent to that address regardless of user intent. Once funds are transferred to the receiving address, the holder of the private key to that account is in complete control of those assets. If funds are sent to a non-existent or inaccessible address, these funds are considered "burned" or lost. Since decentralized blockchains have no central authority in control, there is no authority capable of reversing a mistaken transaction or retrieving mistakenly transferred funds. Since cryptocurrency addresses typically consist of long strings of letters and numbers, the risk of sending funds to the wrong address by mistake is very real. This is another reason why cryptocurrency users minimize the number of transactions to send crypto to the intended recipient—to reduce the chances of an error in a transaction. In my example above, if user A sends the cryptocurrency directly to user C, there is one fewer opportunity for a party to enter the wrong address by mistake.

19. In addition, it is common practice for a crypto user to confirm the recipient address and to conduct a test transaction to that address with a small amount of funds before executing the full transaction. Test transactions are small transactions that are used to confirm the

[6] https://www.bitpanda.com/academy/en/lessons/what-are-transaction-fees-and-why-do-i-need-to-pay-them/

correct recipient address, and that the crypto will be received without any issues. Once the address is confirmed, then it is considered safe to send larger transactions.[7]

The Use of Wallets

The Importance of Wallets

20. Cryptocurrency wallets play an important role in the digital asset ecosystem. Wallets collect data concerning the user's public address, such as balances and transaction history, and aggregate it for the user's review.[8] This allows users to access blockchains in an easy and streamlined manner.

21. Additionally, wallets are used to interact with blockchains. Wallets don't actually hold cryptocurrency. Rather they provide the ability to use the private keys necessary to sign transactions and control the digital assets that are associated with the public address.[9] Protecting the use of private keys is of the utmost importance, as anyone in possession of the private keys controls the contents of that wallet.

Wallet Ownership

22. As the crypto industry has matured, an array of wallet types have been developed to serve users. These wallets can differ in several important ways, such as:

- Hosted vs. Unhosted: Hosted or custodial wallets are hosted by a third party, like an exchange, which stores cryptographic keys for the user. This means that a user instructs the third party to transact on the blockchain on the user's behalf. In an unhosted or non-custodial wallet, the user stores their own keys. Therefore, the user must transact on their own behalf.
- Hot vs. Cold: Hot wallets are connected to the internet, while cold wallets exist offline.
- Software vs. Hardware: Software wallets are applications for devices such as phones and computers. Hardware wallets are actual, physical devices that resemble a USB drive. Hardware devices are plugged into a computer when a user wants to make a transaction.

23. These wallet types are not mutually exclusive. In fact, a wallet can fit into several categories at once. For instance, in the case of popular wallet provider MetaMask, it is a software wallet because it operates as an application for a device. It is also a hot wallet because it is connected to the internet, and an unhosted wallet because it does not control the user's private keys.

24. Different wallet types have different implications concerning wallet ownership. For instance, a hosted wallet is useful to a user who wants the ease of interacting with the blockchain through an exchange. However, this requires outsourcing security over the private keys that control the cryptocurrency to a centralized entity. Therefore, while an

[7] https://dailycoin.com/test-transactions-crypto-why-check-blockchain-transactions/
[8] https://www.investopedia.com/terms/b/bitcoin-wallet.asp
[9] https://crypto.com/university/crypto-wallets

account holder has rights to an amount and type of cryptocurrency, the actual control is with another party. This is akin to a traditional bank account, where a customer has the right to money associated with his/her account, but the funds are possessed by the bank.

25. By comparison, an unhosted wallet provides a user with complete control over cryptocurrency. The owner of an unhosted wallet is in sole control of their private keys. Only this user can access and control the cryptocurrency associated with that private key. Therefore, the user of an unhosted wallet has complete ownership of the contents of that wallet. This is akin to keeping a dollar inside of a wallet in your pocket. The only way to access that dollar is by controlling that wallet.

26. I understand that it has been suggested that Mr. Goldstein may have "shared" ownership of one or more cryptocurrency wallets with third parties. In my experience, shared ownership of cryptocurrency wallets is strongly disfavored and very uncommon.

27. Since private keys prove ownership of cryptocurrency and provide complete control over their movements, the sharing of private keys, while possible, is strongly discouraged and considered a major security risk. Users should avoid ever sharing their private keys with other individuals, because ownership of an account's private key means full control over that wallet's contents.[10] In other words, if user A shares ownership of a cryptocurrency wallet with user B, and then user A deposits millions of dollars of cryptocurrency into the wallet, user B would be able to appropriate user A's cryptocurrency by using the private key to transfer user A's funds out of the "shared wallet" into another cryptocurrency wallet owned solely by user B.

28. As a part of this engagement, I reviewed publications from three of the largest cryptocurrency exchanges by volume and three of the most utilized wallet providers to review mentions of private key security. All of them implore their users to keep their private keys secure and avoid sharing them.[11]

29. I am aware of a few very limited instances when multiple owners of private keys are utilized. When funds are intended to be co-owned or part of a business, multiple-signature (multi-sig) wallets are typically used. Multi-sig wallets operate largely the same as other wallet types, but require the input of multiple private keys to authorize transactions. This setup ensures that no single party can control the wallet's contents without the input of the other party.[12]

30. Whether a transaction from a public address required -signatures can be discerned from the public records associated with the wallet. I have reviewed the transaction history for the two cryptocurrency wallets at issue in this case and I have seen no evidence that either of those wallets is a multi-sig wallet.

[10] https://help.coinbase.com/en/coinbase/getting-started/crypto-education/glossary/private-key
[11] The exchanges reviewed were Binance, Coinbase, and OKX. The wallets reviewed were Trust Wallet, Metamask, and Ledger.
[12] https://www.investopedia.com/multi-signature-wallets-definition-5271193

Transaction History of the Two Addresses at Issue Here

[redacted] *935B*

31. Utilizing open source blockchain explorers, as well as proprietary analytics software, I have examined the transaction history of crypto address 0[redacted]935B ("935B"). This address was created on November 14, 2022, and most recently transacted on February 18, 2025. As of February 24, 2025, the wallet holds approximately $6,781 worth of cryptocurrency. This primarily consists of approximately 5,255 USDT, .365 ETH, and 1 BNB token.

32. I understand that the government has pointed to transactions that occurred in the wallet in February 2025 as evidence that Mr. Goldstein must have owned the wallet. However, based on my analysis of the full transaction history of this wallet, I conclude that the recent transactions in the wallet are consistent with a broader pattern of activity that has occurred in the wallet on a regular basis over a period of several years. There is nothing about the February 2025 transactions that stands out from, or is inconsistent with, this years-long pattern of activity in the wallet.

33. Since inception, 935B has been active, with a pattern of deposits and withdrawals. There have also been multiple multi-week periods without any recorded non-spam activity.[13] The longest of these periods was 52 days, with no recorded activity between February 2, 2024, and March 25, 2024. As of February 24, 2025, the account has engaged in 220 total non-spam transactions with approximately $100,652,868.30 worth of digital assets received, and approximately $100,554,723.30 withdrawn on the Ethereum and Binance Smart Chain.[14] I did not observe the utilization of a multi-signature feature on any of these transactions.

34. The address continues to be active. Some recent transactions of note include a 2,000,000 USDT withdrawal to a Binance deposit address on February 11, 2025, two withdrawals to unhosted wallets on February 18, 2025 of 50,000 USDT and 44,742 USDT, as well as an incoming deposit of 99,997 USDT on February 18, 2025. I understand that the February 11, 2025 withdrawal was made while Mr. Goldstein was incarcerated, and that the February 18, 2025 transactions were made after the government made clear that it was monitoring the wallet.

35. Concerning illicit activity, I have not observed any activity on-chain consistent with asset laundering methods associated with 935B. I also did not observe any direct connections to addresses that show malicious or scam activity. The account interacts regularly with unhosted wallets and centralized exchanges that adhere to a mix of Know Your Customer

[13] Spam crypto activity refers to unprompted and unsolicited deposits of digital assets to a crypto wallet and is analogous to spam or junk e-mail. Spam crypto activity is commonplace.

[14] To limit the activity to non-spam transactions only named tokens with greater than 0 tokens transferred and with value were considered

compliance.[15] Based on these factors, I do not observe any significant steps from the owner of 935B to obfuscate its activity or ownership, or engage in illicit activity.

[redacted] *54E3*

36. Utilizing open source blockchain explorers, as well as proprietary analytics software, I have examined the transaction history of crypto address [redacted]54E3 ("54E3"). This address was created on June 6, 2023, and most recently transacted on February 5, 2025. As of February 24, 2025, the wallet holds approximately $223,120 worth of cryptocurrency. This consists of approximately 221,716 USDT and .5765 ETH.

37. This address has been relatively dormant throughout its existence. The address was funded on June 6, 2023 with 242,410 USDT, with no transactions until February 5, 2025. On that date, the address received .576 ETH (approximately $1,394.51) from an unhosted wallet, and withdrew 22,000 USDT to a separate unhosted wallet.

38. Concerning illicit activity, I have not observed any activity on-chain consistent with asset laundering methods associated with 54E3. I also did not observe any direct connections to addresses that show malicious or scam activity.

39. Based on on-chain data, the sole withdrawal of 22,000 USDT on February 5, 2025 does not indicate suspicious activity even considering the pertinent dates of this proceeding. First, limiting a withdrawal to 22,000 USDT does not alter the public nature of the withdrawal; any withdrawal of any amount would be public. Additionally, 54E3 still held approximately $223,120 worth of cryptocurrency that was available to the address owner on February 5, 2025 which was not withdrawn. Therefore, only a small fraction (approximately 9%) of the total amount of cryptocurrency in the account was moved out of the account on February 5. Moreover, the withdrawal was not made to a brand new, clean wallet, but to a wallet created on October 29, 2024. Based on these factors, I do not observe any significant steps from the owner of 54E3 to obfuscate transaction activity, or to engage in malicious activity.

Jason Trager

[15] Know Your Customer (KYC) compliance is a process designed to prevent financial crimes on a platform by verifying the identity and risk profile of users.

Jason Trager

Senior Director
Blockchain and Digital Assets

1166 Avenue of the Americas
New York, NY 10036
+ 1 (212) 850-5604
Jason.Trager@fticonsulting.com

Education

J.D., Brooklyn Law School (2010)

B.A., University of Maryland, College Park (2007)

Certifications

Certified Blockchain Expert

Certified Cryptocurrency Expert

Certified Cryptoasset AFC Specialist (CCAS)

Chainalysis Investigation Specialist

Chainalysis Reactor

Chainalysis Fundamentals of Cryptocurrency

Associations

ACAMS

Blockchain Council

Wall Street Blockchain Alliance

New York State Bar

Jason Trager is an expert in financial crime investigations, regulations, and compliance concerning digital assets and the blockchain. During his career with FTI, he has overseen investigations into cyber incidents resulting in large scale thefts of cryptocurrency, evaluated compliance and security protocols on behalf of cryptocurrency wallets and exchanges, and conducted due diligence into a blockchain protocol on behalf of Fortune 500 companies. Mr. Trager has analyzed and authored reports concerning the theft, custody, and value of digital assets for use in litigation. He has testified as an expert in the blockchain, cryptocurrency investigations, and illicit activity in both civil and criminal matters.

For more than a decade, Mr. Trager served as a prosecutor in New York City, rising to the position of Chief of Cyber Crimes in the Queens County District Attorney's Office. He managed a team of investigators, attorneys, and forensic accountants in the investigation and prosecution of money laundering through cryptocurrency, theft of digital assets, identity theft and data breaches, ransomware, and darknet trafficking. Mr. Trager co-created the office's cryptocurrency task force, which spearheaded investigations alongside agents from Homeland Security Investigations, the FBI Cyber Crime Task Force, and the New York City Police Department Computer Crimes Unit. During his tenure, Mr. Trager oversaw dozens of blockchain investigations. Utilizing blockchain tracing and digital forensics, these investigations resulted in the successful prosecution of illicit actors, and the seizure of digital assets valued at hundreds of thousands of dollars.

Mr. Trager also worked as a Financial Security Officer and subject matter expert on digital assets, illicit activity, and BSA/AML compliance at BNP Paribas. As Vice President of the Financial Investigations Unit for North America, he advised transaction monitoring teams on the use of blockchain analytics and developed policies and procedures concerning exposure to illicit activity. Mr. Trager served as a digital assets expert for the BNPP Digital Assets Group, where he consulted investment groups on the purchase and sale of digital assets, worked with product development teams to secure newly tokenized assets, and issued briefs to attorneys, compliance officers, and executives on regulatory developments and enforcement actions that concerned digital assets.

During his twelve years as a litigator, Mr. Trager prepped, directed, and cross-examined expert witnesses in numerous court proceedings. These experts ranged in subject matters that included blockchain analytics, valuation, and digital forensics. Mr. Trager has trained in-house detectives on digital assets and blockchain in order to achieve expert witness status. He has also aided in the creation of numerous expert witness reports, and critically examined expert reports submitted by opposing counsels.

Mr. Trager authored the first search warrant in New York State that used blockchain analytics as a basis for probable cause. He also authored his office's official templates for subpoenas and search and seizure warrants for cases concerning digital assets.

At BNP Paribas, Mr. Trager was the lead AML advisor on the bank's first digital bond issuance. He also helped author a guide to the rules and procedures of notifying U.S. regulatory agencies regarding digital asset activity, designed a digital assets focused risk assessment, and regularly provided updates to executives on regulatory developments.

Testimony/Reports

- Declaration, September 24, 2024 - In re: Celsius Network LLC, et al., No. 22-10964; Mohsin Y. Meghji, Litigation Administrator, as representative for the post-effective date debtors v. Wallet Owner 0X10F546A6F4D20D91E5A8506124384759C9F4BC79, et al., United States Bankruptcy Court, Southern District of New York, Case No. 24-03994.
- Testimony, July 30, 2024 -Tobias Kaplan vs. Consensys Software, Inc., JAMS Arbitration Ref.#534000096.
- Testimony, March 5, 2024 - People v. Autumn Clark, et al., Supreme Court State of New York, Indictment No. 270/2024.
- Testimony, October 26, 2023 - Frank Ahlgren, Jr., Elise Leak vs. Frank Ahlgren, III, Copernican LLC, Liquid Publishing LLC, District Court of Travis County, 2D-1-GN- 20-001472.
- Declaration accepted as testimony, June 9, 2023 -In The Marriage of Nadia Zahmoul and Karim Noureddine Zahmoul, No: BV20D08761, London, UK.
- Affidavit, January 31, 2019 - People v. Carlton Vaughn, Criminal Court State of New York, Case no. CR-006205-20QN.
- Affidavit, July 6, 2015 - People v. Edward Gomez et al, Supreme Court State of New York, Indictment No. 1068/2015.
- Testimony, January 24, 2013 - People v. Ramdai Narine, Supreme Court State of New York, Indictment No. 3292/2012.
- Testimony, April 10, 2012 and May 10, 2020 - People v. Derrick Allen, Supreme Court State of New York, Indictment No. 2813/2012.

Cases Prosecuted Utilizing Blockchain/Digital Assets Expert Witness Testimony

— People v. Andre Hyman, Supreme Court State of New York, Indictment No. 711484/2023.

— People v. Nithushan Sachithanantham, Criminal Court State of New York, CR-026327-21QN.

— People v. John Doe, Supreme Court State of New York, Indictment No. 16220002/2022.

Professional Publications, Presentations, and Speaking Engagements

— Knowing the Evolution of Crypto Helps Defenses in Legal Disputes – Bloomberg Law, November 2024

— Bringing Blockchain Due Diligence into Focus Alongside Uptick in Strategic Dealmaking – November, 2024

— AML Compliance and Investigations for Digital Assets – State Street. October 15, 2024.

— Money, Financial Technology, and Blockchain Regulations – Tulane University; Freeman School of Business. April 23, 2025.

— Hot Topics In Digital Evidence: Cryptocurrency and Blockchain – The Advocates' Society. March 5, 2024

— Crypto Investigation Management: Best Practices for Supporting Civil Litigation Strategies – CFAAR. October 12, 2023

— Investigating Cyber Crime in a Digital Assets World - Fordham Law School. February 23, 2023

— Crypto Crime: The Use of Digital Assets in the Criminal World and How to Use Them to Enhance Your Case – NY Prosecutors and NYPD. February 23, 2022

Awards & Recognition

— District Attorney of the Year: Investigations Division 2017

Employment History

— April 2023 – Present: FTI Consulting – Blockchain & Digital Assets, Technology Segment, New York NY - Senior Director

— May 2022 – April 2023: BNP Paribas – Financial Investigations Unit, Digital Assets, New York NY- Vice President

— September 2010 – May 2022: Queens County District Attorney's Office, Queens NY – Chief of Cyber Crimes